REMARKS/ARGUMENTS

Claims 1-23 are pending. Claim 1 stands provisionally rejected on the ground of nonstatutory obvious doubling patenting over Claim 1 of copending Application No. 10/675,496. Claims 1-23 stand rejected under 35 USC 102(e) as anticipated by Shin etal (US Patent 5,967,134).

The Examiner is thanked for the interview today with Mr. Earle Jennings, a patent agent working the GSS Law Group to represent the Applicant in these matters and the copending Application 10/675,496. This paper will summarize the discussion from the Applicant's point of view, as well as provide further details than were available at that time.

Remarks regarding Non-statutory Double Patenting

The Applicant notes that in a response to an Office Action for Application No. 10/675,496 that was filed last week, Claim 1 was cancelled. In the interview today, Mr. Jennings stated that in a response he wrote for the '496 application, which was filed by mail recently, Claims 1-4 were cancelled, and consequently the basis for the provisional rejection had been removed. The Examiner stated that he preferred that a terminal disclaimer be filed, and the Applicant is complying with that request.

Remarks on rejections based upon 35 USC 102(e)

Claims 1-23 stand rejected under 35 USC 102(e) as anticipated by Shin etal (US Patent 5,967,134). The Applicant disagrees with this rejection, and as there are several independent Claims, will argue the rejection arguments for them, with a summary discussion for the dependent Claims.

Here is the central argument Mr. Jennings presented in the interview: Shin discloses excellent technology and many embodiments, is well written, particularly considering the language hurdle of translation from Japanese. And the Examiner is understandable in calling this out as a significant piece of prior art. However, Shin does not disclose stores of shared secrets and the picking of which ones to use. This is a central element of the disclosed invention, as found in the summary of the

invention page 5 lines 1-4: "The challenge may include instructions for the device to use a particular private shared secret stored on the device. The device uses the challenge and designated private shared secret to generate a response." This would be like two childhood friends creating a secure exchange as follows:

> *"Do you remember when I hit you in third grade? Do you remember the girl we were fighting about? Use her name as the key."*

Such a scheme essentially breaks the possibility of an intruder successfully creating a man in the middle attack, because it is very unlikely that the intruder would possess the shared private secret.

Mr. Jennings has since the interview been able to confirm that the initially filed application also discloses the user device storing public shared secrets and/or private shared secrets.

Claim 1 stands rejected as anticipated by Shin (column 8, line 1 to column 10, line 35; column 25, line 65 to column 26 line 43).

> *1. (Currently amended) A method for controlling access to a network, the method comprising the following steps:*
>
> *(a) coupling a user device to a network;*
>
> *(b) transmitting a first response <u>including a particular secret of at least two secrets stored in the user device</u> to the network;*
>
> *(c) generating a second response <u>including the particular secret</u> upon receipt of the first response by the network;*
>
> *(d) comparing the first response and second response; and*
>
> *(e) authenticating the user device if the first response and second response match, and not authenticating the user device if the first response and second do not match.*

The Applicant disagrees with this rejection. Shin does not call out a user device storing at least two secrets and using a particular secret. Consequently, the Examiner is requested to remove this rejection from the Claim.

Claims 2-7 are dependent upon Claim 1.

2. (Currently amended) The method of claim 1 wherein the first response includes a public shared secret as the particular secret.

3. (Currently amended) The method of claim 1 wherein the first response includes a private shared secret as the particular secret.

4. (Currently amended) The method of claim 1 wherein the first response includes a public shared secret and a private shared secret as the particular secret.

5. (Original) The method of claim 1 wherein the second response includes a public shared secret as the particular secret.

6. (Original) The method of claim 1 wherein the second response includes a private shared secret as the particular secret.

7. (Original) The method of claim 1 wherein the second response is generated by the network.

These Claims are dependent upon Claim 1 and inherit its limitations. Shin does not call out a user device storing at least two secrets and using a particular secret. Consequently, the Examiner is requested to remove this rejection from these Claims.

Claim 8 stands rejected as anticipated by Shin (column 8, line 1 to column 10, line 35; column 25, line 65 to column 26 line 43).

8. (Currently amended) A method for controlling access to a network, the method comprising the following steps:

(a) coupling a user device storing at least two secrets to a network;

(b) transmitting a request to the network;

(c) transmitting a challenge including an instruction to use a particular secret of the secrets to the user device;

(d) generating a first response including the particular secret;

(e) transmitting the first response to the network;

(f) generating a second response including the particular secret upon receipt of the first response by the network;

(g) comparing the first response and second response; and

(h) authenticating the user device if the first response and second response match, and not authenticating the user device if the first response and second do not match.

The Applicant disagrees with this rejection. Shin does not call out a user device storing at least two secrets and using a particular secret. Consequently, the Examiner is requested to remove this rejection from the Claim.

Claims 9-14 are dependent upon Claim 8.

9. (Currently amended) The method of claim 8 wherein the first response includes a symmetric public shared secret in the particular secret.

10. (Currently amended) The method of claim 8 wherein the first response includes a symmetric private shared secret in the particular secret.

11. (Currently amended) The method of claim 8 wherein the first response includes a symmetric public shared secret in the particular secret and a symmetric private shared secret in the particular secret.

12. (Currently amended) The method of claim 8 wherein the second response includes a symmetric public shared secret in the particular secret.

13. (Currently amended) The method of claim 8 wherein the second response includes a symmetric private shared secret in the particular secret.

14. (Original) The method of claim 8 wherein the second response is generated by the network.

These Claims are dependent upon Claim 8 and inherit its limitations. Shin does not call out a user device storing at least two secrets and using a particular secret. Consequently, the Examiner is requested to remove this rejection from these Claims.

Claim 15 stands rejected as anticipated by Shin (column 8, line 1 to column 10, line 35; column 25, line 65 to column 26 line 43).

15. (Currently amended) A method for controlling access to a public network, the method comprising the following steps:

(a) coupling a user device to a public network, the network including a server, and the user device stores at least two public shared secrets;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to ascertain one of the public shared secrets as a selected public shared secret stored on the user device;

(e) generating a first response using at least the selected public shared secret;

(f) transmitting the first response to the server;

(g) generating a second response upon receipt of the first response by the server;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the public network if

the first response and second response match, and not authenticating the user device if the first response and second do not match.

The Applicant disagrees with this rejection. Shin does not call out a user device storing at least two public shared secrets and using a particular secret. Consequently, the Examiner is requested to remove this rejection from the Claim.

Claims 16-18 are dependent upon Claim 15.

16. (Original) The method of claim 15 wherein the first response includes a symmetric public shared secret.

17. (Original) The method of claim 15 wherein the second response includes a symmetric public shared secret.

18. (Original) The method of claim 8 wherein the second response is generated by the server.

These Claims are dependent upon Claim 15 and inherit its limitations. Shin does not call out a user device storing at least two public shared secrets and using a particular secret. Consequently, the Examiner is requested to remove this rejection from these Claims.

Claim 19 stands rejected as anticipated by Shin (column 8, line 1 to column 10, line 35; column 25, line 65 to column 26 line 43).

19. (Currently amended) A method for controlling access to a private network, the method comprising the following steps:

(a) coupling a user device to a private network, the network including a server, and the user device stores at least two private shared secrets;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) *processing the challenge to ascertain at least a selected private shared secret stored on the user device;*

(e) *generating a first response using at least the selected private shared secret as one of the private shared secrets;*

(g) *transmitting the first response to the server;*

(h) *generating a second response upon receipt of the first response by the server;*

(i) *comparing the first response and second response; and*

(j) *authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.*

The Applicant disagrees with this rejection. Shin does not call out a user device storing at least two private shared secrets and using a particular secret. Consequently, the Examiner is requested to remove this rejection from the Claim.

Claim 20 stands rejected as anticipated by Shin (column 8, line 1 to column 10, line 35; column 25, line 65 to column 26 line 43).

20. (Currently amended) A method for controlling access to a private network, the method comprising the following steps:

(a) *coupling a user device to a private network, the network including an access control server, and the user device stores at least two private shared secrets and at least two public shared secrets;*

(b) *transmitting an access request from the user device to the server, the access request comprising a first response that includes a selected public shared secret as one of the public shared secrets and a selected private shared secret as one of the private shared secrets, both stored on the user device;*

(c) *invoking the server to generate a second response upon receipt of the first response, the server generating the second response by means of the following steps,*

(i) processing the challenge transmitted to the user device to retrieve the selected public shared secret and the selected private shared secret, and

(ii) processing the selected public shared secret and selected private shared secret to generate the second response;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.

The Applicant disagrees with this rejection. Shin does not call out a user device storing at least two private shared secrets and at least two public shared secrets and using a particular private secret and a particular public secret. Consequently, the Examiner is requested to remove this rejection from the Claim.

Claims 21 and 22 are dependent upon Claim 20.

21. (Original) The method of claim 20 wherein the first response includes a symmetric public shared secret and a symmetric private shared secret.

22. (Original) The method of claim 20 wherein the second response includes a symmetric public shared secret and a symmetric private shared secret.

These Claims are dependent upon Claim 20 and inherit its limitations. Shin does not call out a user device storing at least two private shared secrets and at least two public shared secrets and using a particular private secret and a particular public secret. Consequently, the Examiner is requested to remove this rejection from these Claims.

Claim 23 stands rejected as anticipated by Shin (column 8, line 1 to column 10, line 35; column 25, line 65 to column 26 line 43).

23. (Currently amended) A method for controlling access to a private network,

the method comprising the following steps:

(a) coupling a user device to a private network, the network including an access control server, and the user device stores at least two private shared secrets and at least two public shared secrets;

(b) transmitting an access request from the user device to the server;

(c) transmitting a challenge from the server to the user device;

(d) processing the challenge to retrieve a selected public shared secret and a selected private shared secret stored on the user device;

(e) processing the selected public shared secret and selected private shared secret to generate a first response;

(f) transmitting the first response to the server;

(g) invoking the server to generate a second response upon receipt of the first response by the server, the server generating the second response by means of the following steps,

(i) processing the challenge transmitted to the user device to retrieve the selected public shared secret and the selected private shared secret, and

(ii) processing the selected public shared secret and selected private shared secret to generate the second response;

(h) comparing the first response and second response; and

(i) authenticating the user device to grant access to the private network if the first response and second response match, and not authenticating the user device if the first response and second do not match.

The Applicant disagrees with this rejection. Shin does not call out a user device storing at least two private shared secrets and at least two public shared secrets and using a particular private secret and a particular public secret. Consequently, the Examiner is requested to remove this rejection from the Claim.

Should the Examiner find that the Claims as presented are not in condition for allowance, the Applicant requests that the Examiner contact Earle Jennings or Gregory Smith at the phone number listed below.

Very respectfully submitted,

/Earle Jennings/
Earle Jennings
GSS Law Group
3900 Newpark Mall Rd
Third Floor, Suite 317
Newark, CA 94560

Registration No. 44,804
Phone (510) 742-7417
Fax (510) 742-7419